Rapport de Veille Technologique N°24

Thème : Sécurité
Edition : Juillet - 7/21/2000

DIFFUSION

	Diffusion	Validation
INTERNE APOGEE Communications		
EXTERNE Exemplaire de démonstration		

REDACTION

Rédigé par : **David IMBERT** Le : 7/21/2000 Visa :

Approuvé par : Olivier CALEFF Le : Visa :

AVERTISSEMENT

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles : mailing-lists, newsgroup, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans aucune garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction de ce document.

Les symboles d'avertissement suivants seront utilisés :

- Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire faire encourir un risque sur le système d'information associé.
- Site susceptible d'héberger des informations ou des programmes dont l'utilisation est illégale au titre de la Loi Française.

Par ailleurs, aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur.

AU SOMMAIRE

Le mot de la « Rédaction »

Les mois d'été connaissent généralement une activité ralentie, dans le domaine de la sécurité comme dans les autres domaines. Signalons toutefois la tenue des congrès Defcon et Blackhat à la fin de ce mois de juillet qui regroupent un grand nombre de hackers mais également de spécialistes de la sécurité et d'officiels gouvernementaux.

Par ailleurs, un nouveau type de faille a été identifié, et décrite, dans la fonction C printf ainsi que ses dérivées. L'exploitation la plus importante qui en a été fait à l'heure actuelle concerne le serveur FTP de l'université de Washington.

Pour tout renseignement complémentaire, éventuelles remarques ou suggestions, vous pouvez nous contacter par mail à l'adresse de courrier électronique suivante : veille-sec@apogee-com.fr

1. Produits et Technologies

1.1. Produits

1.1.1. Supervision

TCPView Pro

- **Objet**

  TCPView Pro est un logiciel pour Windows 9x, NT 4.0 et 2000. Edité par la société Winternals Software, il s'agit d'un utilitaire permettant de visualiser l'ensemble des connexions réseaux en cours.

- **Description**

  TCPView peut être comparé à l'utilitaire netstat fourni avec Windows NT et permettant d'afficher la liste des ports UDP et TCP ouverts. TCPView apporte principalement deux fonctionnalités qui font défaut à netstat : La liste des ports est rafraichie à intervals réguliers et le processus auquel appartient chaque port est indiqué.

  La fenêtre de TCPView se divise en deux parties. Dans la moitié supérieure est affichée la liste des ports ouverts sur la machine, associés au processus qui l'utilise, à l'adresse distante lorsqu'une connexion est établie et aux statistiques indiquant la quantité de données reçues et émises.

  La zone inférieure permet de garder une trace des connexions effectuées. Un mécanisme de filtres permet de limiter la quantité d'information affichée afin d'améliorer la lisibilité. Cela permet en particulier d'avoir une visibilité des connexions et non des paquets envoyés ou reçus.
  De même, il est possible de filtrer les adresses ou les processus que l'on souhaite afficher.

  TCPView est un utilitaire extrêmement pratique lorsque l'on a besoin de visualiser les connexions effectuées par une machine et de les associer à une application. Il est également possible de s'assurer du comportement d'applications que l'on soupçonne de transmettre des informations à des sites distants.

- **Complément d'information**

  Winternals http://www.winternals.com

1.1.2. Tunnels chiffrants

Stunnel

- **Objet**

  Stunnel est un logiciel sous license GPL jouant le rôle de passerelle SSL. Il permet ainsi la création de tunnels chiffrés pour des applications ne disposant pas de cette fonctionalité.

- **Description**

  Chaque instance de Stunnel peut agir comme un client ou un serveur SSL. Le mode client accepte des connexion depuis le

port indiqué et redirigeant le flux vers la destination choisie après encapsulation dans un flux SSL, le mode serveur effectuant l'opération inverse en redirigeant le flux SSL vers un service non chiffré.

Le mode serveur est typiquement utilisé sur la machine hébergeant le service accédé et est peut être lancé directement par inetd. Bien qu'il soit tout à fait possible de l'utiliser en conjonction avec TCP Wrapper, ses fonctionalités peuvent être incluses dans Stunnel à la compilation.
Il est également possible de configurer Stunnel comme un proxy redirigeant les connexions après encapsulation dans SSL. Il s'agit du seul mode disponible actuellement sur la version Windows NT.

L'authentification par certificats peut être activée ou non. Il est possible de restreindre les certificats acceptés à ceux stockés sur le serveur. Les certificats des autorités de certifications acceptées sont stockées dans un répertoire du logiciel.

Stunnel est toutefois limité par son mode de fonctionement. Il est en effet impossible de l'utiliser pour sécuriser des protocoles utilisant des connexions multiples dépendant de données hors-bande, tel que ftp. De plus, la version Windows NT ne dispose pas de toute les fonctionalités de la version UNIX. Il est ainsi impossible à utiliser en tant que service et doit être exécuter depuis une fenêtre de l'interpréteur de commandes.

- **Complément d'information**

Stunnel http://www.stunnel.org

1.2. TECHNOLOGIES

1.2.1. Programmation

PORTAGE D'APPLICATION

- **Objet**

eEye Digital Security porte le célebre scanner nmap sur Windows NT.

- **Description**

Le scanner de ports Nmap, considéré comme l'un des plus évolués de sa catégorie était jusqu'ici disponible uniquement sur plate-forme UNIX. eEye annonce avoir réalisé le portage de cet outil sur Windows NT en deux jours. Selon eEye, cette performance démontre qu'il n'est pas plus difficile de créer de bons outils de sécurité open source sur Windows NT que sur d'autres plates-formes.

L'existence de librairies pour Windows NT, telles que Cygnus ou Libnet, offrant une interface de programmation proche de celle disponible sur UNIX facilite grandement le portage d'outils divers par des programmeurs essentiellement habitués à un environnement UNIX. Notons à ce propos que l'utilisation de nmapNT suppose l'installation préalable d'un pilote spécifique permettant un accès direct à l'interface réseau, les pilotes réseaux présents dans Windows NT limitant les possibilités des programmeurs.

- **Complément d'information**

nmapNT http://www.eeye.com/html/Databases/Software/nmapnt.html

1.2.2. Bandeaux publicitaires

EDEXTER

- **Objet**

Les pages des sites web comportent de plus en plus de bandeaux publicitaires qui sont constitués d'images se trouvant sur des sites spécialisés.

- **Description**

Les principaux reproches faits à ces annonces sont le temps de chargement supplémentaire qu'elles imposent ainsi que le traçage des visiteurs des sites les utilisant par la compagnie contrôlant le serveur contenant les publicités. Les détenteurs des sites contenant ces liens sont rétribués au prorata du nombre de requêtes effectuées vers le serveur.

L'idée originale du concepteur de eDexter consiste à utiliser le fichier hosts de la machine afin de remplacer les adresses de ces serveurs de publicité par une adresse inaccessible. Il peut s'agir d'une adresse privée inexistante voire même de l'adresse de bouclage IP. Ainsi le navigateur sera incapable d'accéder à l'image publicitaire. Des listes de tels serveurs sont proposés sur le site afin d'éviter la saisie des très nombreux serveurs concernés.

Le logiciel eDexter intervient comme complément de cette idée. La manipulation précédemment décrite provoque l'apparition de carrés inesthétique et peut provoquer des temps de flottement avec certains navigateurs à la tentative de chargement de l'image depuis un serveur inexistant.
eDexter est un serveur HTTP installé sur la machine et renvoyant à toute requête GET une des images présentes dans le répertoire ad hoc. Il s'agit par défaut d'images de 1 pixel sur 1 pixel mais elles peuvent être remplacées au choix de l'utilisateur.

- **Complément d'information**

eDexter	http://accs-net.com/hosts/

2. INFORMATION ET LEGISLATION

2.1. INFORMATION

2.1.1. Audit

AUDIT DU NOYAU DE LINUX

- **Objet**

  Un projet dont le but est l'audit du noyau de Linux a été créé.

- **Description**

  En tant que système libre dont les sources sont librement accessibles, Linux bénéficie d'une communauté de développeurs assurant des réponses rapides aux problèmes découverts. En revanche, ce mode de développement peut être plus propice à la présence de bogues dans les programmes.

  Le but de ce projet est de mettre à jour les failles de sécurité qui peuvent se trouver dans le noyau avant qu'elles soient exploitées. Il est organisé sous la forme d'une liste de diffusion permettant à chacun de remonter les failles qu'il a pu trouver et de proposer des corrections. Les informations retirées de ce projet devraient également permettre de faire prendre conscience aux développeurs des règles à respecter pour produire du code en limitant les risques de trous de sécurité.

  Les cibles de l'audit sont les noyaux 2.0, 2.2 et le noyau 2.3/2.4 actuellement en cours de développement.

- **Complément d'information**

  Linus Kernel Auditing Project http://www.lkap.org

2.2. LEGISLATION

2.2.1. Responsabilité des hébergeurs de site

LE CONSEIL CONSTITUTIONNEL MODIFIE LA LOI RELATIVE A LA LIBERTE DE COMMUNICATION

- **Objet**

  Saisie par une soixantaine de députés à propos de la loi n° 86-1067 relative à la liberté de communication, le conseil constitutionnel en a éliminé certains alinéas.

- **Description**

  Le conseil constitutionnel avait été saisi par un groupe de parlementaires contestant la validité de plusieurs des ses dispositions, en particulier en ce qui concerne les attributions des moyens de transmission hertziens et le contrôle des opérateurs.

  La majorité des griefs présentés par les députés ont été rejetés et la plus grande partie du texte a été validé. En revanche, bien que cette partie de la loi du 28 Juin ne soit pas concernée par le recours déposé, le conseil constitutionnel a modifié le paragraphe portant sur la responsabilité des hébergeurs de site. En effet, ont été supprimées les dispositions responsabilisant les hébergeurs lorsque « ayant été saisies par un tiers estimant que le contenu qu'elles hébergent est illicite [...] elles n'ont pas procédé aux diligences appropriées ». L'hébergeur n'a plus obligation que de se soumettre aux directives de la justice.

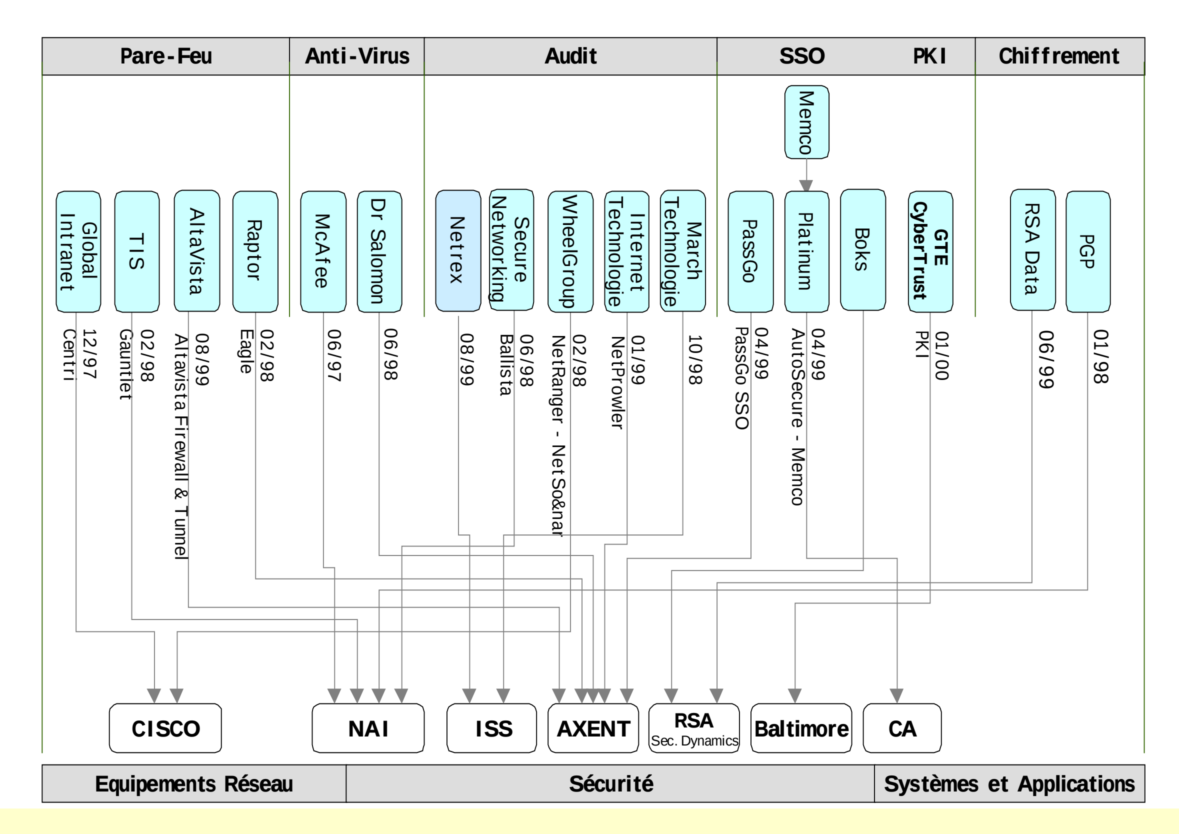
Le motif de cette suppression est l'imprécision du texte original. En conséquence, le principe présent dans la loi du 28 Juin reste applicable pour peu que le gouvernement remanie la loi de façon à combler ces imprécisions.

- **Complément d'information**

Dossier du conseil contitutionnel http://www.conseil-constitutionnel.fr/decision/2000/2000433/

2.3. ALLIANCES

Les différentes alliances - rachats, prises de participation, accords technologiques, … - sont récapitulées au moyen d'un synoptique régulièrement mis à jour.



2.4. LOGICIELS ET SERVICES DE BASE

Les dernières versions disponibles des principaux logiciels du **Domaine Public** sont rappelées dans le tableau suivant. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

Nom	Fonction	Dernière Version officielle	Ancienneté	Apport de la dernière version	Références
Apache	Serveur WEB	1.3.12 au 25/02/2000	5 mois	Alerte CERT Cross Scripting	http://www.apache.org
		2.0a4 au 05/06/2000	1 mois	Version béta	
Bind	Serveur DNS	8.2.2p5 au 12/11/1999	8 mois	Problèmes majeurs de sécurité	http://www.isc.org/products/BIND/
Imap	Serveur IMAP	4.7c2 au 23/02/2000	3 mois	Correction de problèmes	http://www.washington.edu/imap/
INN	Gestionnaire de News	2.2.3 au 20/07/1999	6 mois	Problèmes de sécurité	http://www.isc.org/products/INN/
OpenLdap	Annuaire LDAP	**1.2.11 au 04/07/2000**	**0 mois**	**Correction de problèmes**	http://www.openldap.org/
Majordomo	Gestion de listes de diffusion	1.94.5 au 15/01/2000	6 mois	Problèmes de sécurité	http://www.greatcircle.com/majordomo/
NTP	Serveur de Temps	3_5.93e au 26/04/1998		NTP Version 3 Export	http://www.eecis.udel.edu/~ntp/
		4.0.99k au 20/07/2000	**0 mois**	**NTP Version 4**	
Perl	Langage interprété	5.6.0 au 23/03/2000	2 mois	Nouvelles Fonctionnalités	http://www.perl.com
Php	Langage de scripting WEB	**4.0.1p2 au 30/06/2000**	**0 mois**	**Nouvelles Fonctionnalités**	http://www.php.net/
Pop	Serveur POP/APOP	3.0.2 au 07/04/2000	1 mois	Nouvelles Fonctionnalités et Corrections de bugs	http://www.eudora.com/qpopper/index.html
Procmail	Traitement des Email	3.14 au 22/11/1999	8 mois	Nouvelles Fonctionnalités	ftp://ftp.informatik.rwth-aachen.de/pub/packages/procmail/
Sendmail	Serveur SMTP	**8.11.0 au 19/07/2000**	**0 mois**	**Amélioration de sécurité**	http://www.sendmail.org
SmartList	Gestionnaire de listes de diffusion	3.13 au 31/03/1999	16 mois	Nouvelles Fonctionnalités	ftp://ftp.informatik.rwth-aachen.de/pub/packages/procmail/
Squid	Cache WEB	2.3stable2 au 02/03/2000	4 mois	Problèmes de sécurité	http://squid.nlanr.net/
Wu-Ftp	Serveur FTP	**2.6.1 au 02/07/2000**	**0 mois**	**Vulnérabilités de sécurité**	http://www.wu-ftpd.org

2.5. LOGICIELS DE SECURITE DU DOMAINE PUBLIC

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public (licence GNU GPL) est proposée dans les tableaux suivants. Cette liste sera régulièrement mise à jour.

ANALYSE DE RESEAU ET DE DATAGRAMMES

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
IP Traf	**Statistiques IP**	**2.2.2 au 14/07/2000**	**0 mois**	http://cebu.mozcom.com/riker/iptraf/
Big Brother	Polleur/visualisateur snmp	1.4f au 05/05/2000	2 mois	http://maclawran.ca/bb-dnld/new-dnld.html
Ethereal	**Analyseur multi-protocole**	**0.8.10 au 09/06/2000**	**0 mois**	ftp://ethereal.zing.org/pub/ethereal/
Cheops	Interface visualisation	0.59		http://www.marko.net/cheops/

CONTROLE D'ACCES

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
TCP Wrapper	Contrôle d'accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers/
XinetD	**Inetd amélioré**	**2.1.8.8p8 au 27/06/2000**	**0 mois**	http://synack.net/xinetd/

ANALYSE DE JOURNAUX

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
Autobuse	Analyse syslog	1.13 au 31/01/2000	6 mois	http://www.picante.com/~gtaylor/autobuse/
Analog	Analyse web apache	4.11 au 31/05/2000	2 mois	http://www.analog.cx

GENERATEURS DE DATAGRAMMES

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
FragRouter	Générateur de Fragmentation	1.6 au 21/09/1997		http://www.anzen.com/research/nidsbench/
IPSend	Générateur Paquets IP	2.1a au 17/09/1997		ftp://coombs.anu.edu.au/pub/net/misc/
TcpReplay	Générateur Session TCP	1.0.1 au 19/05/1997		http://www.anzen.com/research/nidsbench/
UdpProbe	Générateur UDP	1.2 au 13/02/1996		http://sites.inka.de/sites/bigred/sw/udpprobe.txt

CONTROLE D'INTEGRITE

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
Tripwire	Intégrité Systèmes NT/UNIX	2.2.1 au 15/12/1999	7 mois	http://www.tripwiresecurity.com/ (version LINUX 5.x, 6.x)
L6	Intégrité Systèmes UNIX	1.6 au 16/10/1998		http://www.pgci.ca/l6.html

SCANNERS

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
Nessus	**Audit de vulnérabilité système**	**1.0.3 au 10/07/2000**	**0 mois**	http://www.nessus.org
Nmap	Audit de vulnérabilité réseau	2.53 au 10/05/2000	2 mois	http://www.insecure.org/nmap
Saint	**Audit de vulnérabilité réseau**	**2.1.2b1 au 24/07/2000**	**0 mois**	http://www.wwdsi.com/saint/
Sara	**Audit de vulnérabilité réseau**	**3.1.5 au 21/07/2000**	**0 mois**	http://www-arc.com/sara
Satan	Audit de vulnérabilité réseau	1.1.1 au 11/04/1995		http://www.cs.ruu.nl/cert-uu/satan.html
Tara (Tiger)	Audit de vulnérabilité système	2.2.6 au 05/06/1999	13 mois	http://www-arc.com/tara
Trinux	Boite à outils	0.7a au 07/03/2000	4 mois	http://www.trinux.org

DETECTION D'INTRUSION / IDS

Nom	Fonction	Dernière Version officielle	Ancienneté	Références
Shadow	Détection d'intrusion Réseau	1.6 au 10/1999	8 mois	http://www.nswc.navy.mil/ISSEC/CID/
Deception ToolKit	'Attrape-mouche'	990818 au 18/08/1999	9 mois	http://all.net/dtk/dtk.html

GARDES-BARRIERES / FIREWALLS

Nom	OS	Dernière Version officielle	Ancienneté	Références
Sinus for Linux	Linux	0.1.5 au 09/12/1999	8 mois	http://www.ifi.unizh.ch/ikm/SINUS/firewall/
DrawBridge	FreeBsd	3.1 au 19/04/2000	3 mois	http://drawbridge.tamu.edu/
IpChain	Linux 2.0	1.3.9		http://www.rustcorp.com/linux/ipchains/
IpFilter	**Filtre de datagrammes**	**3.4.8 au 19/07/2000**	**0 mois**	http://coombs.anu.edu.au/ipfilter/ip-filter.html

RESEAUX PRIVES VIRTUELS / VPN

Nom	Fonction	Dernière Version officielle	Ancienneté	Références	
CIPE	LINUX CIPE Kernel Driver	1.3.0 au		http://sites.inka.de/sites/bigred/devel/cipe.html	☠
FreeS/Wann	LINUX IPSEC	1.0 au 09/02/2000	2 mois	http://www.flora.org/freeswan/	☠
OpenSSL	SSL	0.9.5a au 01/04/2000	3 mois	http://www.openssl.org/	☠
ModSSL	Intégration SSL dans apache	2.6.4 au 01/05/2000	1 mois	http://www.modssl.org	☠
Photuris	Protocole de gestion des clefs	04/02/98		http://www.physnet.uni-hamburg.de/provos/photuris/	☠
SSH	Shell sécurisé (SSH1)	2.1.0 au 12/08/99	9 mois	http://www.ssh.fi/sshprotocols2/	☠
OpenSSH	**Shell sécurisé (SSH1)**	**2.1.1 au 08/06/2000**	**0 mois**	http://www.openssh.org	☠
SSF	Shell sécurisé autorisé (SSH1)	1.2.27.6 au 16/09/99	9 mois	http://info.in2p3.fr/secur/ssf/	
VPS	LINUX Tunnel IP	2.0b2		http://www.strongcrypto.com/	☠
Stunnel	Proxy SSL	3.8 au 23/02/2000	4 mois	http://www.stunnel.org/	

3. NORMES ET PROTOCOLES

3.1. PUBLICATIONS

3.1.1. RFC

Durant la période du 15 Juin au 15 Juillet, **24** RFC ont été publiés, dont **7** ayant trait au domaine de la sécurité.

RFC TRAITANT DE LA SECURITE

Thème	Numéro	Date	Status	Titre
IPSEC	2857	06/00	pStd	The Use of HMAC-RIPEMD-160-96 within ESP and AH
RADIUS	2865	06/00	Std	**Remote Authentication Dial In User Service (RADIUS)**
RADIUS	2866	06/00	Info	RADIUS Accounting
RADIUS	2867	06/00	Info	**RADIUS Accounting Modifications for Tunnel Protocol Support**
RADIUS	2868	06/00	Info	RADIUS Attributes for Tunnel Protocol Support
RADIUS	2869	06/00	Info	RADIUS Extensions
D-H	2875	07/00	pStd	Diffie-Hellman Proof-of-Possession Algorithms

Les abréviations suivantes sont utilisées :
PStd : Proposition de standard Std : Draft Standard Exp : Expérimental Info : Pour information Bcp : Procédure d'utilisation optimale

AUTRES RFC

Thème	Numéro	Date	Status	Titre
CONV	2856	06/00	pStd	Textual Conventions for Additional High Capacity Data Types
BGP	2858	06/00	pStd	Multiprotocol Extensions for BGP-4
TSWTCM	2859	06/00	Exp	A Time Sliding Window Three Colour Marker (TSWTCM)
CONV	2860	06/00	Info	Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority
IP	2861	06/00	Exp	TCP Congestion Window Validation
RTP	2862	06/00	pStd	RTP Payload Format for Real-Time Pointers
MIB	2863	06/00	**Std**	**The Interfaces Group MIB**
MIB	2864	06/00	pStd	The Inverted Stack Table Extension to the Interfaces Group MIB
MIB	2870	06/00	Bcp	Root Name Server Operational Requirements
IP	2871	06/00	Info	A Framework for Telephony Routing over IP
RSVP	2872	06/00	pStd	Application and Sub Application Identity Policy Element for Use with RSVP
IP	2873	06/00	pStd	TCP Processing of the IPv4 Precedence Field
DNS	**2874**	**07/00**	**pStd**	**DNS Extensions to Support IPv6 Address Aggregation and Renumbering**
CMS	2876	07/00	Info	Use of the KEA and SKIPJACK Algorithms in CMS
TELNET	2877	07/00	Info	5250 Telnet Enhancements
PPP	2878	07/00	pStd	PPP Bridging Control Protocol (BCP)

Les abréviations suivantes sont utilisées :
PStd : Proposition de standard Std : Draft Standard Exp : Expérimental Info : Pour information Bcp : Procédure d'utilisation optimale

3.1.2. IETF

Durant la période du 15 Juin au 15 Juillet, **292** DRAFTS ont été publiés, ou mis à jour, dont **50** ayant directement trait au domaine de la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du draft	Date	Titre
AUTH	draft-perlman-strong-pass-00.txt	07/07/2000	Strong Password-Based Authentication Using Pseudorandom Moduli
COPS	draft-ghani-odsi-cops-00.txt	07/07/2000	COPS Usage for ODSI
DNSSEC	draft-ietf-dnsext-message-size-00.txt	06/07/2000	DNSSEC and IPv6 A6 aware server/resolver message size requirements

GSM	draft-haverinen-mobileip-gsmsim-00.txt	19/06/2000	GSM SIM Authentication for Mobile IP
KRBS	draft-thomas-kink-charter-00.txt	11/07/2000	Kerberized Internet Negotiation of Keys
LDAPv3	draft-zeilenga-ldapv3bis-rfc2829-00.txt	07/07/2000	LDAPv3bis Suggestions: Authentication Methods for LDAP
	draft-zeilenga-ldapv3bis-rfc2830-00.txt	07/07/2000	LDAPv3bis Suggestions: Extension for Transport Layer Security
MULTIC	draft-irtf-smug-mcast-policy-00.txt	23/06/2000	Multicast Security Policy
	draft-irtf-smug-data-transforms-00.txt	07/07/2000	Multicast Data Security Transformations: Requirements, Considerations, and Proposed Design
NTP	draft-ietf-stime-ntpauth-00.txt	11/07/2000	Public-Key Cryptography for the Network Time Protocol Version 1
PEPP	draft-sugano-impp-proposal-pepp-00.txt	14/06/2000	Privacy-enhanced Presence Protocol (PePP)
PKIX	draft-adams-cmpaltcert-00.txt	06/07/2000	Alternative Certificate Formats for PKIX-CMP
	draft-ietf-pkix-ldap-schema-00.txt	11/07/2000	Internet X.509 Public Key Infrastructure Additional LDAP Schema for PKIs and PMIs
PROTOC	draft-mrose-bxxp-design-00.txt	05/07/2000	On the Design of Application Protocols
RADIUS	draft-tjoens-aaa-radius-00.txt	13/06/2000	Framework for the extension of the RADIUS(v2) protocol
	draft-congdon-radius-8021x-00.txt	07/07/2000	IEEE 802.1X RADIUS Usage Guidelines
SILC	draft-riikonen-silc-spec-00.txt	28/06/2000	Secure Internet Live Conferencing (SILC), Protocol Specification
	draft-riikonen-silc-ke-auth-00.txt	28/06/2000	SILC Key Exchange and Authentication Protocols
TLS	draft-rozenblit-snmpv3-tls-secmodel-00.txt	06/07/2000	TLS-based security model for SNMP

Les documents à lire en priorité sont mentionnés en caractères gras

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du draft	Date	Titre
AAA	draft-ietf-mobileip-aaa-reqs-04.txt	06/07/2000	Mobile IP Authentication, Authorization, and Accounting Requirements
DHCP	draft-ietf-dhc-authentication-14.txt	06/07/2000	Authentication for DHCP Messages
	draft-ietf-dhc-csr-02.txt	20/06/2000	The Classless Static Route Option for DHCP
DIAMTR	draft-calhoun-diameter-strong-crypto-04.txt	10/07/2000	DIAMETER Strong Security Extension
DOCSIS	draft-ietf-ipcdn-bpiplus-mib-03.txt	23/06/2000	Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus
FCP	draft-kuthan-fcp-01.txt	15/06/2000	Firewall Control Protocol Framework and Requirements
FW	draft-iab-firewall-req-02.txt	12/06/2000	Behavior of and Requirements for Internet Firewalls
GRE	draft-dommety-gre-ext-04.txt	23/06/2000	Key and Sequence Number Extensions to GRE
IDEA	draft-ietf-smime-idea-05.txt	26/06/2000	Use of the IDEA Encryption Algorithm in CMS
IDS	draft-ietf-idwg-data-model-03.txt	15/06/2000	Intrusion Detection Exchange Format Data Model
ISAKMP	draft-ietf-ipsec-notifymsg-03.txt	06/07/2000	Content Requirements for ISAKMP Notify Messages
	draft-vlado-ipsec-keep-alive-01.txt	06/07/2000	Internet Security Association and Key Management Protocol (ISAKMP) Keep-Alive Message exchange
KMP	draft-harney-sparta-gsakmp-sec-02.txt,.ps	13/06/2000	Group Secure Association Key Management Protocol
KRBS	draft-hornstein-snmpv3-ksm-01.txt	13/06/2000	A Kerberos Security Model for SNMPv3
	draft-smedvinsky-dhc-kerbauth-01.txt	10/07/2000	Kerberos V Authentication Mode for Uninitialized Klients
LDAP	draft-behera-ldap-password-policy-02.txt	11/07/2000	Password Policy for LDAP Directories
	draft-zeilenga-ldap-passwd-exop-04.txt	07/07/2000	LDAP Password Modify Extended Operation
MIB	draft-ietf-ipsec-doi-tc-mib-03.txt	14/06/2000	IPsec DOI Textual Conventions MIB
NAT	draft-ietf-nat-app-guide-03.txt	10/07/2000	NAT Friendly Application Design Guidelines
PKIX	draft-ietf-ipsec-pki-req-05.txt	11/07/2000	A PKIX Profile for IKE
PROTOC	draft-mrose-blocks-appldesign-02.txt	16/06/2000	On the Design of Application Protocols
RFC	draft-rescorla-sec-cons-01.txt	19/06/2000	Guidelines for Writing RFC Text on Security Considerations
S/MIME	draft-ietf-smime-seclabel-01.txt	06/07/2000	Implementing Company Classification Policy with the S/MIME Security Label
SASL	draft-zuccherato-9798-3-sasl-01.txt	10/07/2000	ISO/IEC 9798-3 Authentication SASL Mechanism
SDP	draft-ietf-mmusic-sdp-directory-type-01.txt	22/06/2000	Describing session directories in SDP
	draft-rajeshkumar-mmusic-sdp-atm-02.txt	06/07/2000	Conventions for the use of the Session Description Protocol (SDP) for ATM Bearer Connections
SIP	draft-dcsgroup-sip-privacy-02.txt	11/07/2000	SIP Extensions for Caller Identity and Privacy
SMTP	draft-hoffman-rfc2487bis-03.txt	07/07/2000	SMTP Service Extension for Secure SMTP over TLS
SOCKS	draft-ietf-aft-socks-pro-v5-05.txt	27/06/2000	SOCKS Protocol Version 5
X.509	draft-ietf-pkix-time-stamp-09.txt	23/06/2000	Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)
	draft-ietf-pkix-ldap-v3-02.txt	07/07/2000	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3

Les documents à lire en priorité sont mentionnés en caractères gras. Un fond de couleur indique les nouveaux Drafts.

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du draft	Date	Titre
IPv6	draft-ietf-ipngwg-ipv6-2260-00.txt	26/06/2000	IPv6 multihoming support at site exit routers
TUNNEL	draft-thuel-mobileip-tt-00.txt	20/06/2000	Dynamic Home Addressing in Mobile IP using Transient Tunnels
VPN	draft-sanchez-mvpn-00.txt	23/06/2000	Mobile Virtual Private Network

IPv6	draft-soliman-mobileip-hmipv6-00.txt	28/06/2000	Hierarchical Mobile IPv6 and Fast Handoffs
OSPF	draft-giacalone-te-optical-next-00.txt	06/07/2000	Network Engineering Extensions (NEXT) for OSPFv3
INTRNT	draft-ohta-isps-00.txt	07/07/2000	The Internet and ISPs
DNS	draft-senie-inaddr-required-00.txt	07/07/2000	Requiring DNS IN-ADDR Mapping
IP	draft-tsuchiya-mtp-00.txt	10/07/2000	An IPv6/IPv4 Multicast Translator based on IGMP/MLD Proxying (MTP)
IPv6	draft-ietf-ipngwg-scoping-arch-01.txt	27/06/2000	IP Version 6 Scoped Address Architecture
IPv6	draft-ietf-ngtrans-broker-03.txt	07/07/2000	IPv6 Tunnel Broker
MTU	draft-ietf-tcpimpl-pmtud-04.txt	14/06/2000	TCP Problems with Path MTU Discovery
NAT	**draft-iab-nat-implications-08.txt**	**10/07/2000**	**Architectural Implications of NAT**

Les documents à lire en priorité sont mentionnés en caractères gras. Un fond de couleur indique les nouveaux Drafts.

3.2. COMMENTAIRES

3.2.1. RFC

RFC 2874 - DNS EXTENSION TO SUPPORT IPV6 ADRESSES AGGREGATION AND RENUMBERING

Ce document est une proposition d'adaptation du DNS à IPv6. Il modifie le RFC 1886 datant de décembre 1995 qui prévoyait des types d'enregistrement supplémentaire par rapport au DNS IPv4. Le but de ces modifications est d 'améliorer les possibilités de délégation.

La résolution nom vers adresse est effectuée ici à l'aide de l'enregistrement « A6 » qui remplace le type « AAAA ». Il est désormais possible de le renseigner en se référant à un domaine ou un sous-domaine autre de façon à ne renseigner que la partie propre de l'adresse. La définition et l'inscription des domaines en plage d'adresse revêtent alors un aspect obligatoire qui était absent jusqu'alors.

Le nom de domaine spécifique à la résolution des adresses vers le nom devient IP6.ARPA. La notation en est modifiée de façon à faciliter la tâche de l'administrateur. De plus les adresses ainsi définies (et donc délégables) peuvent compter un nombre quelconque de bits.

Enfin, le type d'enregistrement DNAME est créé. Il permet d'effectuer une résolution inverse d'une adresse de sou réseau vers le nom de domaine correspondant. Ces entrés sont en particulier utilisées comme substituts aux requêtes inverses lorsque le mode récursif n'est pas disponible.

Ces nouvelles définitions de type d'enregistrement permettent de définir des zones hiérarchisées et de multiplier les délégations. Toutefois, un profond travail de réflexion et de définition d'architecture DNS est nécessaire avant toute mise en oeuvre à grande échelle étant donnée la complexité à laquelle on peut aboutir si l'on souhaite exploiter toutes les possibilités offertes.

3.2.2. IETF

DRAFT-IAB-NAT-IMPLICATIONS-08.TXT - ARCHITECTURAL IMPLICATIONS OF NAT

Ce document écrit par Tony Hain de Microsoft rappelle les conséquences de la mise en place de translation d'adresse dans un réseau. Il présente en particulier plusieurs sources potentielles de problèmes lors de l'emploi de ce mécanisme dans des réseaux importants.

Le mécanisme de translation d'adresse est le plus souvent utilisé soit pour permettre un accès à un réseau externe lorsque l'on ne dispose que d'un nombre restreint d'adresses utilisables ou pour dissimuler l'adresse d'une machine pour des raisons de sécurité.
Les facilités de conexions qu'il apporte font pour certains de ce mécanisme une alternative à IPv6 dont le dévelopement avait initialement été provoqué par le manque d'adresses disponibles avec IPv4. Pourtant, un certain nombre de fonctionalités sont apportées par IPv6 dont certaines sont justement incompatible avec la translation d'adresses.

Les principaux avantages et désavantages relevés par l'auteur sont résumé ci-dessous :

Avantages du NAT	Désavantages du NAT
Changement d'adressage invisible	Rompt le principe de connexion point à point Incompatible avec IPSEC
Diminutiuon du nombre d'adresses requises	
Partage de charge facilité et transparent	Les points de routage peuvent être source d'incompatibilité
Augmente la durée d'utilisation d'IPv4	Impose des visions DNS différentes à chaque point Peut provoquer des conflits d'adresse
	Icompatibilité avec certaines applications
	Certains cas peuvent compliquer l'évolution vers IPv6

DRAFT-HAVERINEN-MOBILEIP-GSMSIM-00.TXT - GSM SIM AUTHENTICATION FOR MOBILE IP

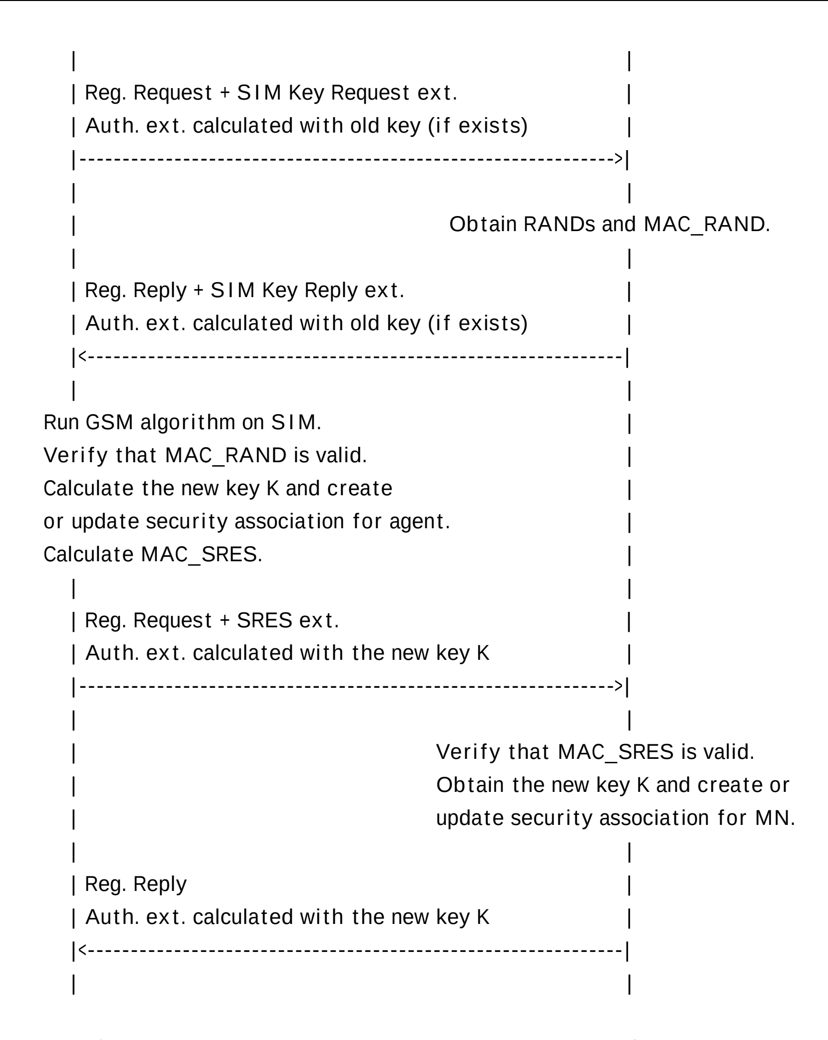
Ce document de H. Haverinen, de Nokia, décrit un protocole d'identification entre un nœud mobile et une passerelle d'accès. Il utilise pour cela les informations comprises dans la carte SIM actuellement contenue dans les téléphones portables.

Le protocole décrit interviens entre le nœud mobile et le point de raccordement de celui-ci au réseau, la propagation des informations d'authentification à l'intérieur du réseau n'est pas pris en compte ici. Le point d'accès devient alors un point critique de l'ensemble.

Le mécanisme décrit dans ce draft utilise les messages d'enregistrement utilisés dans le GSM auquel est rajouté trois extensions (dénommée SIM Key Request, SIM Key Reply et SRES) permettant l'authentification initiale entre les parties ainsi que l'établissement d'une clé temporaire qui sera utilisée dans la suite de la communication. Le principe utilisé dans le mécanisme d'authentification initial proposé est à base de *challenge/response* à l'initiation de la connexion puis signe chaque message avec la clé calculée à l'établissement de la connexion.

Le déroulement d'une connexion authentifiée est reprise ci-dessous :

Mobile Node Mobility Agent



```
   |                                                        |
   | Reg. Request + SIM Key Request ext.                    |
   | Auth. ext. calculated with old key (if exists)         |
   |------------------------------------------------------->|
   |                                                        |
   |                                     Obtain RANDs and MAC_RAND.
   |                                                        |
   | Reg. Reply + SIM Key Reply ext.                        |
   | Auth. ext. calculated with old key (if exists)         |
   |<-------------------------------------------------------|
   |                                                        |
Run GSM algorithm on SIM.                                   |
Verify that MAC_RAND is valid.                              |
Calculate the new key K and create                          |
or update security association for agent.                   |
Calculate MAC_SRES.                                         |
   |                                                        |
   | Reg. Request + SRES ext.                               |
   | Auth. ext. calculated with the new key K               |
   |------------------------------------------------------->|
   |                                                        |
   |                                    Verify that MAC_SRES is valid.
   |                                    Obtain the new key K and create or
   |                                    update security association for MN.
   |                                                        |
   | Reg. Reply                                             |
   | Auth. ext. calculated with the new key K               |
   |<-------------------------------------------------------|
   |                                                        |
```

Il est à noter qu'il s'agit d'un des nombreux drafts publiés par Nokia depuis le début de l'année et se rapportant à la connectivité de nœuds mobiles, que ce soit de façon générale ou comme ici spécifique à la technologie particulière de la téléphonie mobile. Nul doute que cela ne traduise une volonté de continuer à s'imposer sur ce secteur en expansion.

4. ALERTES ET ATTAQUES

4.1. ALERTES

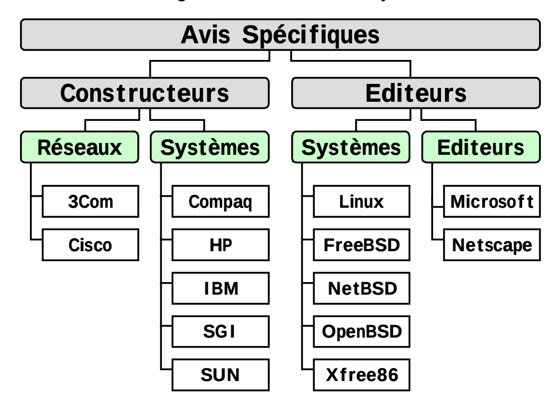
4.1.1. Guide de lecture des avis

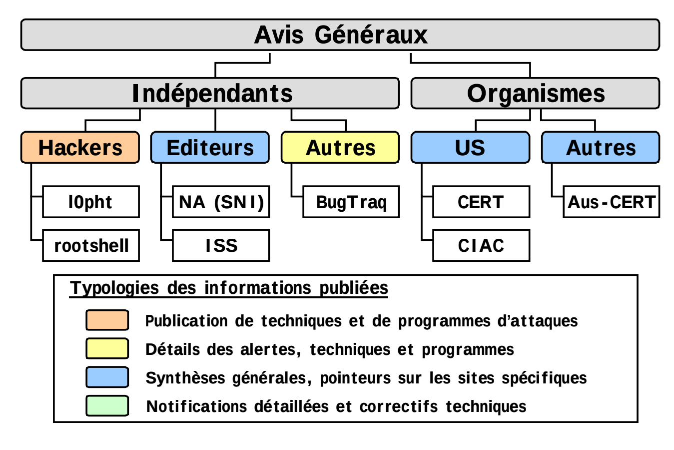
La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

- Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,
- Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme de chartes synthétisant les caractéristiques de chacun des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés. Ces chartes seront régulièrement mises à jour.





L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

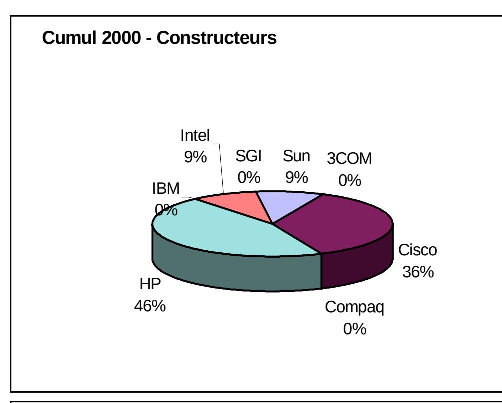
- Recherche d'informations générales et de tendances : Lecture des avis du CERT, du CIAC et du CERT Australien,
- Maintenance des systèmes : Lecture des avis constructeurs associés
- Compréhension et anticipation des menaces : Lecture des avis des groupes indépendants

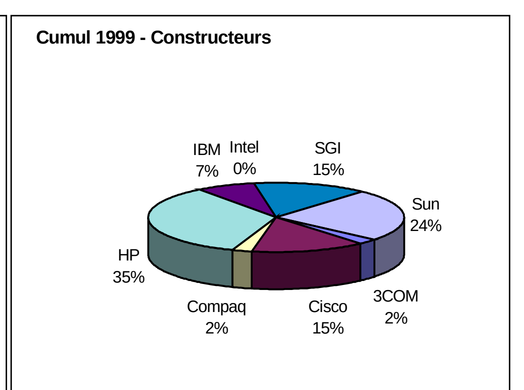
Aus-CERT
CERT
3Com
Cisco
Compaq
HP
IBM
SGI
SUN
Microsoft
Netscape
BugTraq
rootshell
l0pht
NA (SNI)
ISS
NetBSD
OpenBSD
Xfree86
Linux
FreeBSD
CIAC

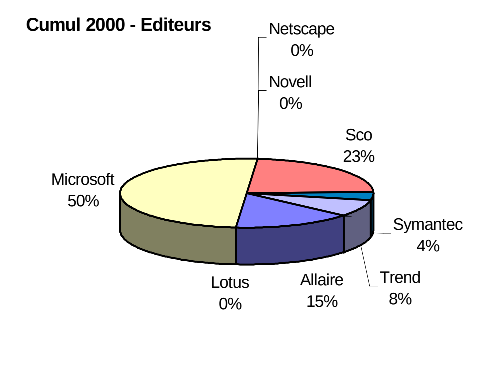
4.1.2. Synthèse des Avis Publiés

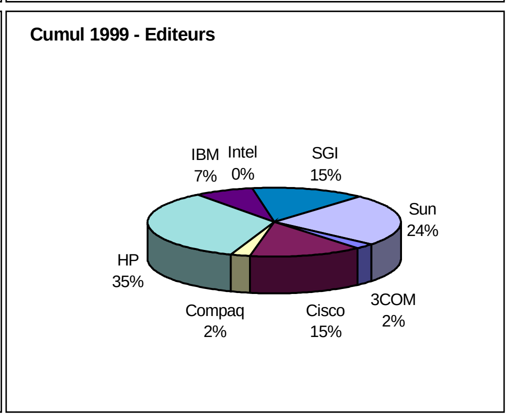
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

	Période	Cumul 2000	Cumul 1999
Organisme	**0**	**19**	**76**
CERT-CS	0	1	4
CERT-CA	0	6	13
CERT-IN	0	1	--
CIAC	0	11	59
Constructeurs	**0**	**11**	**41**
3COM	0	0	1
Cisco	0	4	6
Compaq	0	0	1
HP	0	5	14
IBM	0	0	3
Intel	0	1	--
SGI	0	0	6
Sun	0	1	10
Editeurs	**0**	**26**	**55**
Allaire	0	4	--
Lotus	0	0	--
Microsoft	0	13	55
Netscape	0	0	--
Novell	0	0	--
Sco	0	6	--
Symantec	0	1	--
Trend	0	2	--
Unix libres	**0**	**10**	**54**
Linux (comm.)	0	1	31
Linux RedHat	0	2	--
Linux Debian	0	1	--
Linux SUSE	0	3	--
BSD	0	3	23
Autres	**0**	**25**	**36**
Bugtraq	0	21	--
L0pht	0	1	10
RootShell	0	1	0
X-Force	0	2	26









4.1.3. Avis officiels

Le tableau suivant présente une synthèse des avis de sécurité émis par un organisme officiel et confirmé par l'éditeur du produit ou le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés doivent immédiatement être appliqués.

Fournisseur ou Produit	Titre				URL			
	Référence	Date	Niveau	Origine	Problème	Dommages	Plateforme	Correction
ALLAIRE	**Codes d'exemple dangereux de JRun**				**http://www.allaire.com/handlers/index.cfm?ID=16290&Method=Full**			
	Allaire ASB00-15	23/06	Moyen	Installation par défaut	Présence de servlets de démonstration	Exécution de fonctions non controlées	JRun 2.3.x	Supprimer ces programmes d'exemples. Ils se trouvent dans les répertoires '$JRUN_HOME/servlets' et '$JRUN_HOME/jsm-default/services/jws/htdocs'.
CISCO	**Déni de service 'TCP Reset' sur le dispositif PIX**				**http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml**			
	CISCO CSCdr11711	11/07	Critique	Traitement du paquet TCP RST (Reset)	Absence de contrôle sur l'origine des paquets TCP RST	Rupture par un tiers des connexions établies à travers le PIX	Produits PIX tous modèles utilisant les révisions logicielles antérieures ou identiques aux révisions 4.2(5), 4.4(4), 5.0(3) et 5.1(1)	Les versions 4.4.(5) et 5.1.(2) sont immunes et doivent être installées au plus vite. Une extension de la mémoire vive peut être requise. La lecture de l'avis CISCO est conseillée.
DEBIAN	**Débordement de buffer dans le serveur 'canna'**				**http://www.debian.org/security/2000/20000702**			
	DEBIAN	02/07	Elevé	Paquetage 'canna'	Débordement de buffer dans le traitement de la commande 'SR_INIT'	Acquisition d'un accès distant disposant des privilèges de 'root'	LINUX 2.1	Installer immédiatement la version 3.5b2-24slink1 sur les systèmes utilisant 'canna'.

FREEBSD	**Vulnérabilité dans la pile IP**				**http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-15&msg=20000622215052.D642E37BF12@hub.freebsd.org**			
	FreeBSD-SA-00:23	22/06	Critique	Pile IP	Erreurs d'implémentation	Corruption de données et déni de service	FreeBSD de versions antérieures au 08/06/2000	Appliquer le correctif disponible et recompiler le noyau. ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:23/ip_options.diff
	Erreur de codage dans l'implémentation 'openssh'				**ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:30/sshd.patch.asc**			
	FreeBSD-SA-00:30 CIAC K-058	05/07	Critique	Service 'sshd'	Maintien des privilèges de 'root' lors d'une authentification de type 'UseLogin'	Exécution de commandes sous les privilèges de 'root'	FreeBSD 4.0-RELEASE, 4.0-STABLE, 5.0-CURRENT utilisant le service 'sshd'.	Un correctif est proposé sur le site de l'éditeur: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:30/sshd.patch Il est cependant recommandé d'assurer une mise à jour du système vers l'une des versions 4.0-STABLE ou 5.0-CURRENT récentes, celles-ci contenant la version OpenSSH 2.1.

OPENBSD	**Débordement de buffer dans l'utilitaire 'modp'**				**http://www.openbsd.org/errata.html#mopd**			
	OpenBSD	05/07	Elevé	Utilitaire 'modp'	Débordement de buffer	Non précisés	OpenBSD 2.7	Appliquer le correctif proposé sur les sources de l'utilitaire ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.7/common/018_mopd.patch

HP	**Déni de service contre Web JetAdmin**							
	HPSBUX0006-116	21/06	Elevé	Serveur web intégré	Non disponible	Déni de service	HP Web JetAdmin 6.0 sur Windows NT 4.0 et Windows 2000	Installer la version 6.0.1233, disponible à : http://www.hp.com/cposupport/swindexes/hpwebjetad1880_swen.html
	Vulnérabilité dans TurboIMAGE				**http://jazz.external.hp.com/src/misc/dbutilsec.txt**			
	HPSBMP0006-007	26/06	Critique	DBUTIL	Non disponible	Accès non autorisé	MPE/iX 4.5 et suivants sur HP3000	Un correctif temporaire est disponible sur : http://jazz.external.hp.com/src/misc/dbutil.tar.Z
	Reprise de l'alerte portant sur les vulnérabilités 'ftp'				**http://europe-support2.external.hp.com/**			
	HPSBUX0007-117	11/07	Critique	Service ftp 1 - Commande 'site exec' 2- Fonction système 'setproctitle()'	1- Erreur dans le traitement des arguments - Erreur dans l'appel de la fonction	Exécution de code non sollicité sous les privilèges 'root'	HP-UX 11.00 - Problèmes 1 & 2 HP-UX 10.20 - Problème 2	Deux corrections temporaires sont proposées dont il est recommandé de les appliquer IMMEDIATEMENT: HP-UX 11 : ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.11.0 HP-UX 10.20 : ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.10.20
IBM	**Appels incorrects aux programmes externes dans cdmount**							
	ISS X-Force CIAC K-052	20/06	Critique	Utilitaire cdmount	Mauvais traitement des arguments	Exécution de commandes non autorisées	AIX	Un correctif est annoncé sous la référence IY10903. En attendant la publication de ce correctif, il est recommandé de retirer la permission setuid du fichier '/usr/lpp/UMS/bin/cdmount'.
ISC	**Vulnérabilité dans le client DHCP**				**http://www.isc.org/products/DHCP/**			
	ISC	24/06	Critique	Programme dhclient	Non disponible	Exécution de commandes non sollicitées	dhclient < 2.0 pl 1	Installer la version 2.0 pl 1 dont les sources sont disponibles sur le site de l'ISC.

LINUX REDHAT	**Vulnérabilités multiples dans l'utilitaire 'imwheel'**				**http://www.redhat.com/support/errata/RHSA-2000016-03.html**			
	RHSA-2000:016-03	03/07	Elevé	Utilitaire 'imwheel'	Erreur dans la gestion des liens symboliques	Destruction par un tiers du processus 'imwheel'	Distributions RedHat 6.1 et 6.2 utilisant l'utilitaire 'imwheel'	Désinstaller le paquetage 'imwheel' sur tout système multi-utilisateurs. Les fonctions de gestion de la souris offertes par 'imwheel' sont désormais intégrées au noyau LINUX.
	Gestion incorrecte des fichiers temporaires par 'makewhatis'				**http://www.linuxsecurity.com/advisories/redhat_advisory-525.html**			
	RHSA-2000:041-02	03/07	Elevé	Utilitaire 'makewhatis' du paquetage 'man'	Prédictibilité du nom des fichiers temporaires Erreur dans la gestion des liens symboliques	Modification des permissions et du contenu d'un fichier	Modification des permissions et du contenu d'un fichier	Mettre à jour immédiatement le paquetage incriminé avec la version man-1.5h1-2.5.x disponible sur le site de l'éditeur: ftp://updates.redhat.com/V.V/OS/man-1.5h1-2.5.x.OS.rpm V.V= version soit 5.2 ou 6.0 ou 6.1 ou 6.2 OS = Processeur soit i386 ou alpha ou sparc
LINUX SUSE	**Vulnérabilité dans l'utilitaire 'tnef'**				**http://www.suse.de/de/support/security/suse_security_announce_55.txt**			
	SUSE	10/07	Critique	Utilitaire 'tnef'	Contrôle du répertoire et du nom du fichier décompressé	Ecrasement de fichiers sensibles	SUSE 6.3 et 6.4, potentiellement tout système UNIX utilisant l'utilitaire 'tnef' de version antérieur à la version 0-124	Installer IMMEDIATEMENT la version 0-124 disponible sur le site de l'éditeur: ftp://ftp.suse.com/pub/suse/OS/update/V.V/ap1/tnef-0-124.OS.rpm

MICROSOFT	**Vulnérabilité dans Windows 2000**				**http://www.microsoft.com/technet/security/bulletin/fq00-020.asp**			
	MS00-020	15/06	Critique	Mécanisme de cloisonnement	Erreur d'implémentation	Accès non autorisé	Microsoft Windows 2000, à l'exception de terminal server	Appliquer le correctif proposé http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20836 Attention, ce correctif ne doit pas être appliqué sur les machines utilisées en cluster.
	Exposition de mot de passe dans SQL Server 7.0				**http://www.microsoft.com/technet/security/bulletin/fq00-035.asp**			
	MS00-035	15/06	Elevé	Mode d'authentification	Stockage du mot de passe administrateur en clair	Vol de mot de passe	SQL Server 7.0, service pack 1 et 2	Un nouveau correctif est proposé. http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21546
	Inefficacité du correctif MS00-031				**http://www.microsoft.com/technet/security/bulletin/fq00-031.asp**			
	MS00-031	17/06	Elevé	Librairie 'ism.dll'	Mauvais traitement des arguments	Acquisition d'informations	Internet Information Server 5.0	Un nouveau correctif est disponible. http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21671
	Insuffisance du correctif sur les fichiers '.chm' sous IE				**http://www.cert.org/advisories/CA-2000-12.html**			
	CERT CA-2000-12	19/06	Elevé	Système d'aide Microsoft	Fonction VBS Windows.showHelp() Méthode 'Shortcut' de l'objet HHCtrl	Exécution de code non sollicité par le biais d'une page WEBréférençant un fichier d'aide piégé.	Internet Explorer 5.0	Microsoft a annoncé ne pas avoir l'intention de produire une deuxième version du correctif.
	Nouveau correctif pour la vulnérabilité de 'Media Encoder'				**http://www.microsoft.com/technet/security/bulletin/fq00-038.asp**			
	MS00-038	20/06	Elevé	'Windows Media Encoder'	Mauvais traitement des requêtes	Déni de service	Microsoft Windows Media Encoder 4.0 et 4.1	Appliquer le nouveau correctif proposé. http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21904
	Incompatibilité des version 56 bits et 128 bits d'Outlook				**http://support.microsoft.com/support/kb/articles/Q263/3/05.ASP**			
	Microsoft	22/06	Moyen	Librairie 'crpt32.dll'	Non disponible	Blocage du système	Windows NT 4.0	Appliquer le correctif fourni : - x86 US : http://www.microsoft.com/downloads/release.asp?ReleaseID=21600 - x86 Fr : http://www.microsoft.com/downloads/release.asp?ReleaseID=21610 - Alpha Fr : http://www.microsoft.com/downloads/release.asp?ReleaseID=21611

MICROSOFT	**Téléchargement automatique de fichiers '.cab' par IE**				http://www.microsoft.com/technet/security/bulletin/fq00-042.asp		
	MS00-042 CIAC K-057	29/06	Critique	Défaut de conception	Téléchargement de fichiers sans confirmation de l'utilisateur	Déni de service par écrasement de fichier	Internet Explorer 4.x et 5.x	Un correctif est disponible. Après son application, un fichier signé par Microsoft est traité comme tout autre fichier et le site distant ne peut choisir le chemin de destination du fichier téléchargé. http://www.microsoft.com/windows/ie/download/critical/patch8.htm our s'installer, ce correctif nécessite IE 4.01 SP 2 ou IE 5.01.
	Vulnérabilité SQL 7.0 'Stored Procedure Permissions'				http://www.microsoft.com/technet/security/bulletin/fq00-048.asp		
	MS00-048 - Q266766	07/07	Elevé à critique	Procédures stockées sous SQL Serveur 7.0	Erreur de conception dans le traitement des permissions	Exécution d'une procédure stockée non autorisée en exécution	Systèmes Windows utilisant SQL Serveur 7.0	Appliquer les correctifs disponibles sur le site de l'éditeur - Intel: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22470 - Alpha: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22469
NORTON	**Vulnérabilités dans NAV pour Exchange**				http://www.securiteam.com/windowsntfocus/Norton_Antivirus_for_Exchange_allows_infected_attachments_to_pass_through.html		
	Securiteam	16/06	Critique	1 - Architecture du produit 2 - Traitement des fichiers '.zip'	1 - Fonctionnement "ouvert par défaut" - Débordement de buffer	Inefficacité de la protection du produit	Norton AntiVirus pour Exchange 1.5 et 2.0	Norton annonce que ce problème sera corrigé dans la version 2.01.
NOVELL	**Problème de filtrage des URL sous BorderWare 3.x**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-07-01&msg=s964b5eb.025@cpl-mail1.cpl.novell.com		
	Novell via Bugtraq	07/07	Critique	Fonction de filtrage des URL	Caractères encodés non traités	Court-circuit des filtres	BorderWare 3.0 et 3.5	Dans son message, le support NOVELL confirme l'existence du problème sur les versions 3.0 et 3.5. Un correctif est annoncé en cours d'établissement.
PANDA SOFTWARE	**Existence d'un port d'administration ouvert à tous**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-15&msg=41256901.003D5E29.00@mailgw.backupcentralen.se		
	Bugtraq	17/06	Critique	Console d'administration distante	Absence de protection	Accès non autorisé	Panda Antivirus pour Netware 2.0, sur Netware 5.0 et 5.1	PandaSoftware a annoncé la disponibilité d'un correctif, référencé M6/A00.

SGI	**Vulnérabilité dans Workshop 2.6.x**							
	SGI CIAC K-056	20/06	Critique	Outil 'cvconnect'	Non disponible	Accès en écriture non autorisé	WorkShop 2.6.x	Installer la version 2.7 du WorkShop pour les version supportées d'IRIX. (6.2 et supérieures). Il est également possible de limiter les droits d'exécution du programme à l'administrateur.
SUN	**Exécution de code arbitraire via le serveur Java WEB**				**http://www.foundstone.com/FS-071000-5-JWS.txt**			
	FS-071000-5-JWS	10/07	Elevé	Application de démonstration 'bboard'	Configuration par défaut du serveur	Exécution à distance de code arbitraire	Java Web Server toutes versions en environnement NT et Solaris	Appliquer immédiatement les recommandations décrites dans le document SUN, et en particulier, éliminer tous les exemples (dont bboard) et détruire l'association '/servlet invoker' dans le fichier de configuration des machines de production. http://www.sun.com/software/jwebserver/faq/jwsca-2000-02.html
VIRUS	**Nouveau virus 'vbs'**				**http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_STAGES.A&VSect=T**			
	Trend Micro	17/06	Critique	Virus	Propagation par messagerie, ICQ et IRC	Engorgement de messagerie	Microsoft Windows	Mettre à jour les logiciels antivirus.
WU FTP	**Vulnérabilité dans Wu-ftp**				**http://www.securiteam.com/unixfocus/Updated_WuFTPd_packages_available.html**			
	Securiteam CERT CA-2000-13	22/06	Critique	Commande 'SITE EXEC'	Mauvaise vérification des arguments	Accès root non autorisé	Wu ftp 2.6.0 et antérieur	Le code source d'un correctif par l'équipe maintenant Wu-ftp est disponible : ftp://ftp.wu-ftpd.org/pub/wu-ftpd/quickfixes/apply_to_2.6.0/lreply-buffer-overflow.patch

4.1.4. Alertes Non Confirmées

Les alertes présentées dans le tableau de synthèse suivant ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une confirmation de la part de l'éditeur ou du constructeur. Ces informations autorisent la mise en place d'un processus de suivi et d'observation.

Fournisseur ou Produit	Titre				URL			
	Référence	Date	Niveau	Origine	Problème	Dommages	Plateforme	Correction
APACHE	**Problème dans le module perl CPAN Apache::ASP v1.95**				**http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-07-08&msg=20000711033856.17708.qmail@securityfocus.com**			
	Bugtraq	10/07	Elevé	Script d'exemple 'source.asp'	Filtrage des caractères d'échappement	Ecriture de fichiers dans le répertoire contenant le script	Plateformes utilisant APACHE et le module Apache::ASP v1.95	Télécharger la dernière version du script 'source.asp' sur les systèmes de développement et détruire ce script sur tous les serveurs de production. http://www.nodeworks.com/asp/
BEA	**Exposition des fichiers sources par Weblogic**				**http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-15&msg=2153DBA073F0D311911100B0D01A826F05BA13@mail.foundstone.com**			
	Foundstone via Bugtraq	21/06	Moyen à élevé	Traitement des URL	Contournement du traitement pages dynamiques	Obtention d'informations	BEA WebLogic 3.1.8, 4.0.x, 4.5.x, 5.1.x	Une modification du fichier de configuration consistant à supprimer la définition d'un module de traitement par défaut et à le déclarer explicitement pour chaque extension à traiter est proposée. Des explications détaillées sont disponibles sur : http://www.weblogic.com/docs51/admindocs/lockdown.html
BIG BROTHER	**Vulnérabilité exposant les fichiers du système**				**http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-07-08&msg=00071110185100.01380@sj-soc-wks1.priv.nuasis.com**			
	Nuasis via Bugtraq	11/07	Critique	Script 'bb-hostsvc.sh' de l'interface WEB de gestion	Absence de controle préalable à l'assignement de la variable HOSTSVC.	Visualisation d'un quelconque fichier	Tout système hébergeant le produit Big Brother de version antérieure ou égale à la version 1.4h	Un correctif est disponible sur le site Big Brother http://www.bb4.com/download.html
	Vulnérabilité exposant les fichiers du système				**http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-07-08&msg=20000711231139.6331.qmail@web2001.mail.yahoo.com**			
	Bugtraq	11/07	Critique	Service WEB 'bbd'	Gestion des fichiers de status	Visualisation d'un quelconque fichier	Tout système hébergeant le produit Big Brother de version antérieure ou égale à la version 1.4h	Aucune correction n'est actuellement annoncée.

CHECKPOINT	**Déni de service sur la version NT de Firewall-1 4.0 et 4.1**				http://www.securiteam.com/securitynews/CheckPoint_Firewall-1_DoS__SMTP_.html			
	SecureXpert SX-20000620-3 via Security Team et Bugtraq	02/07	Critique si avéré	Proxy SMTP (Module SMTP Security server)	Erreur dans le traitement de flux contenant une succession de caractères nuls (valeur binaire 0)	Déni de service par consommation excessive de temps CPU	Firewall-1 4.0 et 4.1 en environnement NT	Aucun avis d'alerte officiel n'a été transmis par Checkpoint. Aucune solution palliative ne peut être proposée en dehors de la désactivation temporaire du proxy !
MICROSOFT	**Nouvelle vulnérabilité dans Internet Explorer**				http://www.securiteam.com/windowsntfocus/Force_Feeding_files_to_Internet_Explorer.html			
	Securiteam	26/06	Critique	Internet Explorer	Non disponible	Téléchargement forcé de fichiers	Internet Explorer 5.0 et 5.1	Aucun correctif n'est disponible pour l'instant.
	Déni de service sur de nombreux services de Windows 2000				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-29&msg=Pine.LNX.3.96.1000630161841.4619A-100000@fjord.fscinternet.com http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-29&msg=Pine.LNX.3.96.1000630161935.4619B-100000@fjord.fscinternet.com			
	SecureXpert SX-20000620-1 et SX-20000620-2 via Bugtraq	01/07	Critique si avéré	Services TCP/7 (echo), TCP/9 (discard), TCP/21 (ftp), TCP/23 (telnet), TCP/7778 UDP/53 (DNS), UDP/67 (bootp), UDP/135 (epmap) UDP/137 (netb-ns), UDP/500 (isakmp), UDP/1812(radius), UDP/1813 (radiusa), UDP/2535, UDP/3456	Erreur dans le traitement de flux contenant une succession de caractères nuls (valeur binaire 0)	Déni de service par consommation excessive de temps CPU	Windows 2000	Microsoft n'a pas encore publié d'avis concernant ces alertes. Dans l'attente d'un complément d'information, il est conseillé de désactiver les services non strictement utiles sur les serveurs Windows 2000.
	Exécution de code contenu dans un DLL sous EXCEL				http://www.nat.bg/~joro/excel2.html			
	G.Guninski via Bugtraq	11/07	Elevé	Excel 2000	Fonction REGISTER.ID	Exécution du code contenu dans la librairie passée en paramètre de la fonction.	Mis en évidence sur Excel 2000 en environnement Windows 98	Aucun correction n'est disponible à ce jour.

NETSCAPE	**Débordement de buffer dans Enterprise Server pour NetWare**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-22&msg=A5F256C2C72FD411BCD600508B65FE6A02B783@nm-exch-cph.internal.n-m.com			
	Bugtraq	26/06	Critique	Traitement des URL	Débordement de buffer	Exécution de code non sollicité	Netscape Enterprise Server 5.0 et 5.1 pour NetWare	ppliquer le Service Pack 1 disponible pour Enterprise Server 5.1 : http://support.novell.com/servlet/filedownload/pub/e51sp1.exe
	Exposition du mot de passe administratif de SuiteSpot				http://www.securiteam.com/securitynews/Netscape_Administration_Server_Password_Disclosure.html			
	Securiteam	11/07	Elevé	Fichier 'admpw'	Accessibilité en lecture	Exposition du mot de passe chiffré	Annoncé sur tout environnement utilisant le service Administration Server installé avec SuiteSpot	Netscape recommande d'invalider l'accès en écriture à ce fichier dans son manuel d'installation, ce qui n'est pas fait lors de l'installation du service. L'accès en lecture reste semble-t-il indispensable pour le bon fonctionnement du service.
NOVELL	**Problème d'authentification sous BorderWare 3.0**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-07-01&msg=06256915.00591E18.00@uprrsmtp2.notes.up.com			
	Bugtraq	08/07	Critique	Utilitaire 'ClientTrust'	Absence de contrôle	Court-circuit du mécanisme d'authentification	Annoncé sur Borderware 3.0	A ce jour, cette alerte n'est pas confirmée par Novell. Ce problème, mis en évidence sur une version obsolète, n'a validé sur la version 3.5 courante.
QMAIL	**Débordement de buffer dans le paquetage 'vpopmail'**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-29&msg=395BD2A8.5D3396A7@secureaustin.com			
	Bugtraq	01/07	Critique	Programme 'vchkpw' assurant l'authentification des utilisateur	Débordement de buffer	Exécution distante de code non sollicité sur le serveur pop	Toute plateforme UNIX utilisant QMAIL et l'extension 'vpopmail' de version antérieur à la version 4.8	Installer immédiatement le paquetage 'vpopmail' version 4.8a sur tout système utilisant cette fonctionnalité. http://www.inter7.com/vpopmail/
SAWMILL	**Exposition du mot de passe administrateur**				http://www.securiteam.com/securitynews/Sawmill_file_and_password_exposure.html			
	Bugtraq	28/06	Critique	Sawmill	Non disponible	1 - Exposition du début de tout fichier lisible par l'ensemble des utilisateurs du système. 2 - Acquisition du mot de passe administrateur de Sawmill	Sawmill 5	Aucun correctif n'est disponible à ce jour.

SSH	**Problème de gestion des tickets Kerberos dans SSH 1.2.27**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-29&msg=200007010511.BAA16944@syrinx.oankali.net			
	R.Silverman via Bugtraq	01/07	Elevé	SSH 1.2.27 compilé avec l'option Kerberos	rédictibilité du nom et de la localisation du fichier contenant le ticket.	Acquisition du ticket et usurpation d'identité	Plateformes utilisant SSH 1.2.27 en environnement Kerberos	L'auteur de l'alerte propose un correctif à appliquer sur les sources de SSH 1.2.27. Il est cependant conseillé de remplacer cette version par la version 1.2.28 corrigeant ce problème.
VERITAS	**Vulnérabilité dans Volume Manager**				http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-15&msg=Pine.LNX.4.20.0006161311110.24059-100000@whip.twistedpair.ca			
	Bugtraq	16/06	Critique	Script de démarrage	Permissions laxistes du dcript d'arrêt du service	Exécution de commandes en mode privilégié	Volume Manager 3.0.x sur Solaris inférieur à 8	Auncun correctif n'est disponible actuellement. Il est possible de rajouter la commande 'umask 022' dans le script de démarrage de Volume Manager afin d'éviter que n'importe qui puisse modifier le fichier '/var/opt/vmsa/logs/.server_pids'.
WINPROXY	**Diverses vulnérabilités**				http://www.securiteam.com/windowsntfocus/WinProxy_vulnerable_to_an_exploitable_buffer_overflow.html			
	Bugtraq	28/06	Critique	1 - Commande 'USER' du proxy POP3 2 - Proxy HTTP	1 - Débordement de buffer 2 - Non disponible	1 - Exécution de code non sollicité 2 - Déni de service	Winproxy 2.0 et 2.0.1	Utiliser la version 2.0.2 http://www2.comco.ne.jp/~sin/WinProxy/

4.1.5. Bulletins d'Information

Le tableau suivant récapitule les bulletins d'information publiés par les organismes officiels de surveillance.

Thème	Titre			URL
	Référence	Date	Objet	Contenu
APACHE	Publication d'un article portant sur la sécurisation			http://apachetoday.com/news_story.php3?ltsn=2000-06-29-003-01-NW-LF
	Apache	04/07	Sécurisation	Un article détaillant les principes de sécurisation du serveur WEB 'apache' en environnement UNIX vient d'être publié sous le titre 'Securing your Web page with APACHE". Une excellente présentation du modèle de sécurité intégré dans Apache permet de comprendre l'importance de l'ordonnancement de certaines déclarations dans le fichier de configuration 'httpd.conf'. Comme toujours, la lecture de ce remarquable article est vivement conseillée.
ATTAQUES	Etude sur l'utilisation d'ICMP pour sonder les systèmes			http://www.sys-security.com/archive/papers/ICMP_Scanning.pdf
		03/07	Technique d'attaque	Une étude fort intéressante portant sur l'utilisation du protocole ICMP en tant qu'outil de sondage (scanning) de systèmes distants est disponible. Chaque technique d'exploitation d'ICMP fait l'objet d'un chapitre détaillant le principe de mise en oeuvre mais aussi la parade susceptible d'être mise en oeuvre au niveau des dispositifs de filtrage amont. La lecture de cette étude est fortement conseillée en notant cependant que la plupart des techniques exposées sont désormais bien connues.
AXENT	Disponibilité de la Security Update 4 pour ESM			http://www2.axent.com/swat/News/Advisory.asp?id=2000-056
	Axent	13/07	Mise à jour	La mise à jour 'ESM Security Update 4' est disponible sur le site AXENT. Celle-ci contient différentes évolutions et nouvelles fonctionnalités trop nombreuses pour être résumées. Le lecteur se reportera à la liste des évolution disponible sur le site de l'éditeur.
AXIDIA	Rachat par le groupe Américain SCIENT			http://www.scient.com/news/articles/article60.asp
	Scient	07/07	Rachat	SCIENT, intégrateur de sites e-business vient d'officialiser le rachat de la SSII française Axidia. Créée en 1995, Axidia intervient notamment dans le domaine de la Sécurité des réseaux. Notons que les accès au site WEB d'Axidia sont tous redirigés sur le site de SCIENT.
BT	Licenses sur l'utilisation de liens hypertexte			http://www.theregister.co.uk/content/1/11450.html
	The Register	30/06	Utilisation de brevet	British Telecom a annoncé posséder un brevet applicable à l'utilisation de liens hypertextes. Ce brevet a été déposé en 1976, avant la séparation de British Telecom et de la poste britannique. BT réclame à chaque fournisseur d'accès américains une licence d'utilisation. Il est difficile de prévoir l'issue de cette affaire, toutefois elle permet aux opposants aux brevets sur les logiciels de fournir de nouveaux arguments.
BULLSOFT	Changement d'identité sous le nom d'EVIDIAN			http://www.bull.fr/securinews/courant/35-01_1.html
	Bull	07/07	Changement de nom	Un nouveau nom, Evidian, un nouveau slogan, net.confidence, et une nouvelle raison sociale, BullSoft renaît sous de nouvelles couleurs et devient une filiale indépendante détenue majoritairement par Bull.

Catégorie	Titre / Source	Date	Type	Lien / Résumé
CERT	**Danger des clients de discussion**			http://www.cert.org/incident_notes/IN-2000-08.html
	CERT IN-2000-08	22/06	Avis d'information	Le CERT a publié une rapport d'incident rappelant les dangers que présente l'utilisation de clients de discussion, particulièrement les clients IRC. Les risques induits sont principalement de deux ordres : - Ces clients peuvent contenir des vulnérabilités tels que des débordements de buffer ou des erreurs de configuration amenant ou facilitant une intrusion sur le poste de l'utilisateur. - L'utilisation de ce mode de communication par des utilisateurs non sensibilisés est un vecteur de "social engineering" connu et exploité par les pirates informatiques. De plus ces canaux de diffusion sont utilisés par des programmes tels que des chevaux de Troie ou les récents virus pour se propager.
CHECKPOINT	**Reprise par le CERT de l'avis sur Firewall-1**			http://www.cert.org/vul_notes/VN-2000-02.html
	CERT VN-2000-02	19/06	Bulletin d'alerte	L'avis de Checkpoint concernant un déni de service dans Firewall-1 a été repris par le CERT sous la référence VN-2000-02.
CNIL	**Lancement de trois nouveaux chantiers de reflexion**			http://www.internet.gouv.fr/francais/frame-actualite.html#cnil
	CNIL	08/07	Reflexion sur l'utilisation d'Internet.	La CNIL lance trois nouveaux chantiers de réflexion concernant l'internet. La Commission nationale de l'informatique et des libertés (CNIL), par la voix de son président Michel Gentot, a annoncé qu'elle ouvrait trois grands chantiers de réflexion autour de l'internet et venait de proposer la création, pour les sites, d'un label européen de protection des données. - Le premier chantier est celui de la "cyber surveillance" des salariés dans l'entreprise : "(...) les messages électroniques reçus ou envoyés peuvent être conservés et lus par d'autres que leurs destinataires naturels" prévient la Commission. -Le deuxième chantier de réflexion concerne la diffusion de décisions de justice nominatives. "Ces arrêts et jugements peuvent comporter les noms des personnes et parfois leur adresse, ils peuvent être accessibles par des moteurs de recherche (...)", explique Michel Gentot. -Le troisième chantier ouvert par la CNIL est celui de l'utilisation commerciale de ses propres données sur internet.
COUNTERPANE	**La Lloyd's assure les clients de la société de B.SCHNEIER**			http://news.cnet.com/news/0-1005-200-2232221.html?tag=st.ne.1002.thed.ni
	CNET	11/07	Accord avec une société d'assurance	B.SCHNEIER, CEO de la société de service et conseil COUNTERPANE, annonce que ses clients pourront bénéficier d'une assurance couvrant les dommages généré par une attaque. Le coût de cette assurance est de $20 000/an pour une couverture plafonnée à $1 Million et de $75 000/an pour un plafond de $10 Million de perte.
CRYPTOGRAPHIE	**Présentation pédagogique de l'échange DH (Diffie/Hellman)**			http://www.securityportal.com/topnews/dhkeyexchange20000706.html
	SecurityPortal	06/07	Présentation d'algorithme	Un article présentant avec de nombreuses illustrations l'échange clef Diffie Hellman est proposé sur le site SecurityPortal. Ce schéma cryptographique est couramment employé dans les systèmes de chiffrement car performant et autorisant une initialisation aisée. Il est à noter que la présentation proposée s'appuie sur les définitions et les mécanismes d'IPSEC.
DNS	**Vulnérabilité des serveurs principaux de l'internet**			http://news.cnet.com/news/0-1005-200-2073583.html?tag=st.ne.1002.bgif.ni
	CNET	16/06	Etude sur les serveurs utilisés	Selon les informations recueillies par Jim Hu et Evan Hansen, plusieurs des serveurs DNS principaux de l'internet utiliseraient d'anciennes versions de BIND et seraient donc vulnérables à différentes attaques pour lesquelles existent des correctifs, plusieurs permettent de modifier les bases de données du DNS. Rappelons que plusieurs vulnérabilités découvertes récemment supposent pour être exploitées que de fausses informations DNS soient reçues par les cibles des ces attaques.

INTERPOL	**Projet commum possible avec la start-up AtomicTangerine**			**http://web.lexis-nexis.com/more/cahners-chicago/11407/6039428/3**
	Atomic Tangerine	07/07	Accord de coopération	La firme de conseil Atomic Tangerine - émanation du SRI - pourrait coopérer avec Interpol pour définir et mettre en place une version avancée du système de veille et d'alerte NetRadar. La création d'un réseau d'alerte permettrait d'accélérer l'échange d'informations concernant le 'cybercrime'. NetRadar est déjà utilisé sur le site SecurityPortal pour cibler les évènements critiques: http://www.securityportal.com/topnews/netradarews/netradarews.html
ISS	**Disponibilité de la X-Press Update 3.8**			**https://www.iss.net/update/InternetScanner**
	ISS	27/06	Mise à jour	ISS a publié la mise à jour 3.8 de son outil de test de vulnérabilité Internet Scanner. Celle-ci intègre la détection d'un débordement de buffer dans le pare-feu Gauntlet ainsi qu'un autre débordement de buffer dans le serveur DNS BIND.
	Mise à jour pour System scanner			
	ISS	29/06	Mise à jour	La X-Press Update 8 pour System Scanner 4 est disponible. Cette mise à jour inclue de nouveaux tests pour Solaris 2.6 et 7 ainsi qu'une nouvelle politique de sécurité pour AIX 4.3. Cette mise à jour est accessible par la mise à jour automatique de System Scanner.
JURIDIQUE	**Problème de la revente des fichiers d'information**			**http://www.droit-technologie.org/2_1.asp?actu_id=962791024&month=7&year=2000**
		12/07	Analyse juridique	L'annonce de la revente au enchère des fichiers d'information collectés par les sites en ligne 'ToySmart.com' et 'Boo.com' par leurs créanciers fait la une des journaux d'information Américains. Une analyse vient d'être publiée qui présente les mécanismes juridiques susceptibles d'être mis en place en Europe pour éviter de telles 'dérives'.
KERBEROS	**Reprise par le CIAC de l'avis du CERT**			**http://www.ciac.org/ciac/bulletins/k-051.shtml**
	K-051	16/06	Bulletin d'alerte	Le CIAC a réémis sous la référence K-051 l'avis du CERT concernant des débordements de buffer dans Kerberos.
MICROSOFT	**Avis du CERT sur les extensions cachées**			**http://www.cert.org/incident_notes/IN-2000-07.html**
	CERT IN-2000-07	20/06	Avis d'information	Dans une nouvelle note d'information, le CERT rappelle le danger des extensions cachées de Windows et les moyens de les afficher. Rappelons que ces extensions cachées ont été fortement utilisées par les récents virus VBS.
	Article sur le développement d'un 'rootkit' Windows			**http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-07-08&msg=396C75FE157.B4E7SOLARECLIPSE@192.168.0.1**
	SecurityFocus	13/07	Technique d'attaque	Un article détaillé sur le développement d'un 'rootkit' spécifique à l'environnement Windows vient d'être publié. La technique utilisée s'appuie sur la possibilité de charger dynamiquement un gestionnaires de périphérique dans le noyau des systèmes Windows 9x. Il est ainsi possible d'intercepter nombre de fonctions systèmes et de prendre le contrôle du poste à distance. Trois articles portant sur cette technique - LKM ou Loadable Module Kernel - ont déjà été publiés et sont accessibles sur le site 'http://www.infowar.co.uk/thc/'.

NAI	**Publication de correctifs pour Gauntlet 5.0**			**ftp://ftp.tis.com/gauntlet/patches/5.0/cluster.BSDI.patch** **ftp://ftp.tis.com/gauntlet/patches/5.0/cluster.HPUX.patch** **ftp://ftp.tis.com/gauntlet/patches/5.0/cluster.SOLARIS.patch** **ftp://ftp.tis.com/gauntlet/patches/5.0/x-gw.patch**
	NAI	27/06	Correctifs	NAI a publié des correctifs pour la version 5.0 de son pare-feu Gauntlet. La résolution d'un débordement de buffer ayant déja fait l'objet d'un correctif isolé est notamment inclus.
	Publication de correctifs pour Gauntlet 5.5			**ftp://ftp.tis.com/gauntlet/patches/5.5/cluster.HPUX.patch** **ftp://ftp.tis.com/gauntlet/patches/5.5/cluster.SOLARIS.patch** **ftp://ftp.tis.com/gauntlet/patches/5.5/ldapauth.patch** **ftp://ftp.tis.com/gauntlet/patches/5.5/smap.patch**
	NAI	27/06	Correctifs	AI a publié des correctifs pour la version 5.5 de son pare-feu Gauntlet. Notons que le correctif intitulé ldapauth.patch avait déja été publié. Celui-ci corrige un problème d'installation sur plate-forme Solaris.
NSI	**Changement de la méthode d'authentification**			**http://www.networksolutions.com/help/guardian.html**
	NSI	30/06	Authentification des clients	Suite aux problèmes de vols de noms de domaine, Network Solutions a annoncé que les mises à jour des informations concernant les noms de domaine enregistrés seraient vérifiés par un retour d'e-mail à la place de la simple vérification de l'expéditeur par le champs 'From'. Il est également question que le partenariat de NSI avec Verisign soit mis à profit pour fournir une authentification forte au propriétaire d'un domaine.
OUTILS	**Etude des limitations des systèmes de détection d'intrusion**			**http://all.net/journal/ntb/IDSstructure.html**
	F. Cohen	05/07	Analyse sur les IDS	Un article portant sur les limites des outils de détection d'intrusion (IDS) a été publié par Fred Cohen courant Mai. Publié à l'état de Draft, cet 'essai' met en évidence, ou plutot démontre, l'incapacité intrinséque des outils IDS à détecter toutes les attaques: interdépendance actions, volume du nombre d'événements signifiants à mémoriser, limitations propres aux machines de Turing ... Le chapitre intitulé 'Roll-Up' propose une excellente synthèse des techniques exploitables à chaque niveau d'abstraction d'un système. Nous conseillons la lecture, à tête reposée, de cet article quasi-philosophique et passé inapercu.
	Senna Spy Trojan Generator			**http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SENNASPY.2K&VSect=T**
	Trend	10/07	Outils d'attaques	Dans la liste des nouveaux virus et chevaux de Troie, l'éditeur TREND annonce la prise en compte de la signature de 'TROJ_SENNASPY.2K'. La lecture attentive de la fiche technique revèle l'adresse du site de l'auteur de ce générateur de chevaux de Troie, adresse visible dans la copie d'écran proposée ! Un rapide survol du site permet de découvrir divers outils complémentaires dont 'Senna Spy One EXE Maker' (un concateneur d'exécutables), 'Senna Spy Internet Worm Generator' (un générateur de vers), 'Senna Spy FTP Server' (un service ftp masqué). Un grand merci à TREND pour avoir divulgué cette adresse jusqu'alors ignorée ...
PASSWORDS	**Publication d'une liste de 'mots de passe par défaut'**			**http://www.securityparadigm.com/defaultpw.htm**
	Bugtraq	10/07	Mots de passe par défaut	Une liste des mots de passe utilisés par défaut dans les équipements et logiciels a été publiée au format 'CSV' dans la liste Bugtraq. Cette liste, qui contient 797 mots de passe, est régulièrement mise à jour sur le site de l'auteur.

QUOVA	**Une société américaine sonde l'Internet**			**http://www.securityfocus.com/news/56**
	SecurityFocus	11/07	Exploration de l'Internet	n article publié par SecurityFocus annonce qu'une société Américaine est en train de sonder activement l'Internet provoquant une avalanche d'alarmes sur les systèmes de détection d'intrusion. La société Quova précise qu'elle utilise les techniques de sondage ICMP et traceroute afin de renseigner une base de donnée utile à ses services de consultant. Il est à noter que si les domaines quova.com, quova.net et quova.org sont tous enregistrés par la même société californienne, aucun site WEB n'est semble-t-il accessible qui puisse permettre de confirmer les dires de l'article.
REDHAT	**Correctifs pour Emacs**			**ftp://ftp.redhat.com/redhat/updates/6.2/SRPMS/emacs-20.7-1.src.rpm**
	RedHat	16/06	Publication de correctifs	Suite à la vulnérabilité dans Emacs concernant les communications inter-processus, RedHat a publié un correctif concernant les distributions 6.x de RedHat. Les utilisateurs d'une distribution 5.x doivent mettre à jour vers une version 6.x.
	Publication d'un paquetage comportant le noyau 2.2.16			**ftp://updates.redhat.com/6.2**
	Red Hat	22/06	Nouveau noyau	RedHat a publié sous forme de paquetage RPM le noyau 2.2.16. Rappelons que cette version du noyau de Linux est immune à une vulnérabilité susceptible d'impacter tout programme setuid.
SPYWARES	**Liste de logiciels suspectés de masquer leur installation**			**http://grc.com/optout.htm** **http://grc.com/oo/spyware.htm**
		05/07	Liste de logiciels « suspzct »	Une excellente liste des logiciels, dits 'SPYWARES' car ayant pour finalité l'espionnage des habitudes de l'utilisateur d'un système, est proposée sur le site WEB de Steve. Cette liste contient le nom de 6 sociétés oeuvrant explicitement dans le domaine de l'analyse et de la mesure d'audience: - Aureate /Radiate (Synthèse N°9 du 31/03/1999) - Conducent TimeSink (Synthèse N°1 du 23/07/1999) - TransCom Beeline - Comet Cursor - GoHip - Web3000 Rappelons que ces 'outils' sont, pour la plupart, chargés sans information ni consentement de l'utilisateur à l'occasion de l'installation d'un logiciel anodin, un Freeware ou un Shareware en général. Les techniques utilisées sont proches de celles mises en oeuvre par des codes malicieux de type chevaux de Troie.
VIRUS	**Site de descriptions de virus**			**http://www.coderz.net/zulu/viruses.htm**
	Zulu	21/06	Site informatif	Ce site, visiblement mis en place par l'auteur des virus présentés, propose des analyses de plusieurs virus dont le récent ShellScrap, également connu sous le nom de STAGES.A. Cette analyse, très complète et comprenant le code source commenté permet de bien comprendre les mécanismes utilisés dans les derniers virus.

VULNERABILITE	Politique de contrôle de la diffusion des informations			http://www.wiretrip.net/rfp/policy.html
	RFP	04/07	Politique de divulgation des informations	L'auteur de nombreuses alertes de sécurité "Rain Forest Puppy", connu sous l'acronyme 'RFP', vient de publier une proposition de politique de contrôle de la diffusion des vulnérabilités. Ce document relance la polémique entre les tenants de la diffusion 'immédiate et totale' - Full disclosure - et ceux de la diffusion 'contrôlée'. La proposition actuelle, élaborée avec l'aide de personnalités du monde de la sécurité - Aleph1, Weld Pond, Russ Cooper -, suggère une approche de type 'contrôlée' comportant cependant de nombreux échappatoires: l'initiateur de l'alerte (ORIGINATOR) contacte l' éditeur du produit (MAINTAINER) qui dispose de 48h pour répondre. L'éditeur dispose ensuite de 5 jours ouvrés (comprenant les 48h de délai de réponse !) pour corriger le problème. A l'issue de ce délai, ou en l'absence de réponse, l'initiateur de l'alerte peut publier toutes les informations en sa disposition. Cette initiative, la première dans ce domaine, pourrait conduire à disposer de canaux d'information régulés donc plus fiables et moins bruités.

4.2. ATTAQUES

4.2.1. Attaques

UTILISATION DES CHAINES DE FORMATAGE DANS LA FONCTION PRINTF

- **Objet**

La fonction de la bibliothèque C *printf*, ainsi que les fonctions dérivées, utilise des chaînes d'échappements permettant le formatage des données ainsi que l'accès à des variables. Certaines conditions d'utilisation de ces fonctions conduisent à interpréter une chaîne transmise par l'utilisateur.

C'est une faille de ce type qui est exploitée dans la récente alerte portant sur Wu-ftp et pour laquelle les rapports du CERT/CC indiquent une grande activité.

- **Description**

Ce type de vulnérabilités permet d'accéder à la pile du système visé en dehors des zones réservées aux variables réservées au traitement des données entrées. Comme pour un débordement de buffer, le but est de modifier la valeur d'un pointeur du programme de façon à ce qu'un code transmis soit exécuté. Ce code consistant généralement à ouvrir un interpréteur de commande accessible par l'attaquant.

En utilisation normale la fonction printf accepte un nombre variable d'arguments. Le premier est une chaîne de caractères permettant de décrire les paramètres suivants. Ceux-ci sont alors interprétés différemment selon les formats indiqués. Les caractères de cette chaîne ne correspondant pas à une indication de formatage sont copiés ou affichés directement.

C'est ce mécanisme qui permet par exemple d'afficher correctement les différentes représentations numériques utilisables dans un programme.

Lorsque la chaîne à traiter ne comporte que du texte, il est courant qu'elle soit placée en argument unique. Dans la mesure où la chaîne en question ne comporte effectivement que du texte sans caractère d'échappement provoquant un traitement de paramètres, le résultat est conforme à ce qui est attendu. Toutefois, lorsque cette chaîne de caractères est transmises par un élément extérieur au programme, il se peut qu'elle contienne de telles séquences d'échappements.

La présence de ces séquences n'étant pas prévue, il n'existe pas de variable correspondante dans la mémoire. La fonction traitera alors comme argument les données présentes dans la pile mémoire. Il peut s'agir de données comme d'adresses de retour qui sera utilisée pour pointer une zone exécutable.

Il est ainsi possible d'obtenir le contenu de la pile mémoire pour peu que le résultat soit retourné à l'utilisateur. Les informations ainsi recueillies sur l'organisation de la mémoire du programme peuvent permettre à un attaquant de déduire les adresses auxquelles il devra placer ses codes d'attaque. Il n'est alors pas nécessaire de posséder une version du logiciel afin de « tracer » son exécution.

De plus, il est possible par l'utilisation du format particulier %n d'écrire dans la mémoire à une adresse de son choix, ou presque. Ce format à pour effet non pas de traiter l'argument fourni comme une donnée à afficher mais inscrit à l'adresse fournie en paramètre le nombre de caractères affichés par la fonction jusqu'à ce point.

exemple :

```
int n ;
printf(« AAAA%n » , &n) ;
```

n vaut alors 4.

L'exploitation de cette fonction consiste à placer l'adresse à laquelle on souhaite placer des données dans la chaîne transmise et à placer le nombre de caractères d'échapement nécessaire pour atteindre le buffer dans lequel est placé cette chaîne dans la fonction contenant l'appel à *printf*.

Il semble que le nombre de programmes susceptibles de contenir des fonctions vulnérables et mal employées soit important. En effet, l'exploitation n'ayant été imaginé ou tout au moins publié que récemment, les dévelopeurs se sont attachés à éviter les eccueils connus. Heureusement, les conditions d'une utilisation aboutissant à l'exécution de code sur la machine cible sont suffisemment restrictives pour limiter les exploitations les plus dangereuses.

- **Complément d'information**

Article de Lamagra Argamal dans Bugtraq	http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-06-22&msg=20000624195754.3020.qmail@fiver.freemessage.com